UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

United States of America,

Plaintiff,

v. Case No. 1:15cr109

Richard Stamper, Judge Michael R. Barrett

Defendant.

OPINION & ORDER

This matter is before the Court upon Defendant's Motions to Compel Discovery. (Docs. 56, 79). The Government has filed Responses (Docs. 61, 82), and Defendant has filed a Reply (Doc. 86). Also before the Court are Defendant's Motion for Reconsideration (Doc. 63) and Motion for a *Franks* Hearing (Doc. 67). On January 22, 2018, the Court held a hearing on the pending motions. (Doc. 94). Following the hearing, the parties provided the Court with Supplemental Memoranda. (Docs. 95, 96).

To the extent that the Government has provided the discovery requested in Defendant's first Motion to Compel (Doc. 56), that motion is DENIED as MOOT.

I. BACKGROUND

Defendant Richard Stamper has been charged with receipt and possession of child pornography in violation of 18 U.S.C. § 2252(a)(2), (a)(4), (b)(1) and (b)(2). These charges stem from an investigation conducted by Special Agents with the Federal Bureau of Investigation ("FBI") which led to the discovery of a child pornography website known

as “Playpen.” The Playpen website was operating on an internet network known as the Tor network, which allows users to hide identifying information such as Internet Protocol addresses (“IP addresses”). At the hearing, Special Agent Daniel Alfin explained:

> The Tor network changes things. So when you access a regular website -- and let's say I go to amazon.com because I want to buy something. When I connect to amazon.com, if I was to do so from my home in Florida, amazon.com would see my IP address assigned to my home in Florida, and they would have a log and a record of that.
>
> So law enforcement, if they were investigating me, could later go to amazon, ask for that IP address, and then eventually they could find my physical address in Florida.
>
> When someone uses the Tor network to access a regular website, their IP address is now masked. If I access a regular website, you can think of my communication as going directly from my home to amazon.com. But now if I go through the Tor network, my communications no longer go directly to amazon.com. Now they are going to bounce around three different computers somewhere all around the word. So my communication could go from my house in Florida to a computer in Georgia, to a computer in France, to a computer in Germany, and then it will go to amazon.com. So when I'm using the Tor network, I can still access amazon.com, but amazon.com doesn't know I'm in Florida. They just see that IP address in Germany.
>
> So typically when you use the Tor network, your home IP address is masked.

(Doc. 94, PAGEID # 647-48).

Based on information from foreign law enforcement, the FBI was able to locate the computer server which hosted the Playpen website. The FBI seized the website and began operating it from a government-controlled server located in Virginia.

FBI agents then obtained a search warrant from a magistrate judge in the Eastern District of Virginia which authorized the use of a “network investigative technique” (“NIT”) to be deployed on the computer server. (Doc. 33-1, Attachment A) (“the NIT warrant”).

The NIT warrant provided that once the NIT was deployed on the computer server, it would obtain information from the activating computers. (Id.) Activating computers are the computers of users or administrators who log in with a user name and password to the Playpen website. (Id.) Each time a user or administrator logged in, the NIT attempted to cause the activating computer to send specific information to a government-controlled computer located in the Eastern District of Virginia. (Doc. 33-1, NIT Search Warrant Aff. ¶36). This information included:

> 1. the activating computer's IP address, and the date and time that the NIT determines what that IP address is;
>
> 2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other activating computers, that will be sent with and collected by the NIT;
>
> 3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
>
> 4. information about whether the NIT has already been delivered to the activating computer;
>
> 5. the activating computer's Host Name;
>
> 6. the activating computer's active operating system username; and
>
> 7. the activating computer's media access control ("MAC") address.

(Doc. 33-1, NIT Search Warrant Aff. ¶ 31).

As a result of the NIT warrant, the FBI discovered that on February 3, 2015, a user registered for an account on the Playpen website using the username "billnyepedoguy." (Doc. 32-1, Residential Search Warrant Affidavit, ¶ 27). The Government explains that according to the statistics section of this user's profile, the user "billnyepedoguy" had been actively logged into the website for a total of four hours, one minute and 57 seconds,

between February 3, 2015 and March 4, 2015. (Doc. 32-1, Residential Search Warrant Affidavit, ¶ 27). The FBI also identified the IP address and MAC Address used by "billnyepedoguy" to log into the Playpen website; and determined "billneypedoguy" used the host name of "badass" and log-on ID of "richard." (Id., ¶ 28).

The FBI was able to determine that the IP address associated with the user "billnyepedoguy" was operated by the internet service provider Time Warner Cable. (Doc. 32-1, Residential Search Warrant Affidavit, ¶ 34). Through an administrative subpoena served on Time Warner Cable, the FBI identified Defendant as the subscriber of the IP address. (Doc. 32-1, Residential Search Warrant Affidavit, ¶ 35). In September of 2015, law enforcement agents obtained a search warrant from a magistrate judge in this district for Defendant's home. The agents seized a laptop which contained images of child pornography. (See Def. Hr'g Ex. 7, Doug Rodin Report of Examination).

By one court's count, Defendant was one of more than a hundred defendants who were implicated by the NIT warrant. *See United States v. Horton*, 863 F.3d 1041, 1045 (8th Cir. 2017). In the current motions, Defendant seeks additional discovery from the government regarding the NIT itself; asks this Court to reconsider its denial of a previous motion seeking to suppress the evidence gathered as a result of the NIT warrant; and seeks a *Franks* hearing based on an alleged false statement made in the affidavit in support of the NIT warrant application.

II. ANALYSIS

A. Motion to Compel Discovery (Doc. 79)

Defendant seeks to compel the government to disclose the "exploit" component of

the NIT. There are four primary components to the NIT: (1) unique identifier generator, which runs on the Playpen server and generates and saves a unique identifier; (2) exploit software, which allows the NIT payload to run; (3) NIT code (or "payload"), which runs in the computer's browser and sends back information to the government; and (4) data logger, which runs on a separate government server and logs the data received from the NIT from the computer. (Def. Hr'g Ex. 1, Dr. Matthew Miller Report, p. 3-4, 5). The Government has provided three of the components to Defendant. Defendant is only seeking a fourth component: the code for the exploit. Defendant maintains that without the exploit code, it is impossible to determine if the government was able to introduce the payload to the computer as it claims; whether the government accurately determined the IP address, MAC address, operating system, host name and Log-on ID; and whether the files containing child pornography were actually placed on the computer by Defendant.

Under Federal Rule of Criminal Procedure 16(a)(1)(E), the government is required to permit inspection of items within its possession, custody, or control if (1) the item is material to preparing the defense; (2) the government intends to use the item in its case-in-chief at trial; or (3) the item was obtained from or belongs to the defendant. In this instance, the parties dispute whether the exploit code is material to the defense preparation.

"It is a defendant's burden to make a prima facie showing of materiality in order to obtain disclosure of a document under Rule 16." *United States v. Dobbins*, 482 Fed.Appx. 35, 41 (6th Cir. 2012) (quoting *United States v. Phillip*, 948 F.2d 241, 250 (6th Cir. 1991)). The Sixth Circuit has defined materiality in this manner:

> Materiality under Rule 16 has not been authoritatively defined in this Circuit. However, the Supreme Court has determined that "defense" within the meaning of Rule 16 means the "defendant's response to the Government's case in chief." *United States v. Armstrong*, 517 U.S. 456, 462 (1996). Therefore, the rule applies only to 'shield' claims that 'refute the Government's arguments that the defendant committed the crime charged.' ... It follows that information which does not counter the government's case or bolster a defense is not material "merely because the government may be able to use it to rebut a defense position." *United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir. 1993). Rather, there must be an indication that pre-trial disclosure would have enabled the defendant to "alter the quantum of proof in his favor," not merely that a defendant would have been dissuaded from proffering easily impeachable evidence. *Id*. In assessing materiality, we consider the logical relationship between the information withheld and the issues in the case, as well as the importance of the information in light of the evidence as a whole. *See id*.

United States v. Lykins, 428 Fed.Appx. 621, 624 (6th Cir. 2011).

Defendant appears to have an uphill battle in demonstrating materiality: the majority of courts have denied motions to compel the government to produce the entire NIT source code. *United States v. Harney*, No. CR 16-cr-38, 2018 WL 1145957, at *11 (E.D. Ky. Mar. 1, 2018); *United States v. Spicer*, No. 1:15-cr-073, 2018 WL 635889, *3 (S.D. Ohio Jan. 31, 2018); *United States v. Gaver*, 3:16-cr-088, 2017 WL 1134814, *5 (S.D. Ohio Mar. 27, 2017); *United States v. Tippens*, No. 3:16-cr-5110, Doc. 106, at 28 (W.D. Wash. Nov. 30, 2016); *United States. v. McLamb*, 220 F.Supp.3d 663, 676 (E.D. Va. Nov. 28, 2016); *United States v. Jean*, No. 5:15-cr-50087, 2016 WL 6886871, *7 (W.D. Ark. Nov. 22, 2016); *United States v. Cruz-Fajardo,* No. 1:16-cr-14, 2017 WL 3634278, at *4 (N.D. Ga. Aug. 23, 2017); *United States v. Matish*, 193 F.Supp. 3d 585, 600 (E.D. Va. Jun. 2, 2016).

Defendant cites to two instances in which the same court found that the NIT source code was material to preparing the defense: *United States v. Michaud*, No. 3:15-cr-5351

(W.D. Wash. May 25, 2016) (transcript of oral ruling at Doc. 56-2) and *United States v. Tippins*, Case No. 3:16cr5110 (W.D. Wash. Mar. 16, 2017) (copy of order at Def. Hr'g Ex. 2C).

Defendant explains that the request for production of the complete NIT information is particularly compelling in this case because discrepancies have been discovered in three categories of information gathered by the NIT: (1) the MAC Address; (2) the operating system; and (3) time stamps on files. Defendant explains further that these discrepancies suggest that the NIT was not functioning as the government claimed. At the hearing, Defendant presented the testimony of Dr. Matthew Miller. Miller testified that in order to determine what caused these discrepancies, it is necessary to examine the exploit code of the NIT. (Doc. 94, PAGEID #121). Miller testified that in order to determine if the exploit was functioning properly, it would need to be tested in a variety of settings, and the testing done by the government was insufficient. (Doc. 94, PAGEID #121-22).

The first discrepancy identified by Defendant is the MAC address. Special Agent Daniel Alfin testified at the hearing that the MAC address:

> helps narrow down the computer, just like the host name and the user name. In a particular residence, there can be multiple computers, there can be multiple people living there. So it's another piece of identifying information that, in some instances, can help narrow down the device that was accessing the Playpen website.

(Doc. 94, PAGEID #659). Defendant explains that the MAC address collected by the NIT does not match the MAC address of Stamper's laptop. Defendant argues that this discrepancy indicates that there is something wrong with the exploit, or the exploit had a

bad interaction with the computer's operating system.

Based on the testimony presented at the hearing, this discrepancy in the MAC address does not show that the exploit code is material.[1] Special Agent Alfin testified: "The IP address is the most important piece of information here. That's what we use to ultimately determine the physical location of someone's residence." (Doc. 94, PAGEID #659). Alfin also testified that Internet Service Providers maintain logs and records of who is using a particular IP address on a particular date and time. (Doc. 94, PAGEID #647). There is no dispute as to the validity of the IP address in this case. Alfin testified:

> This is the real IP address that the defendant was using when the NIT identified him. As I testified earlier, when you access the internet through

[1]At the hearing, one possible explanation for the discrepancy in the MAC addresses was offered: Defendant was using a virtual machine. Special Agent Doug Roden testified that the MAC address collected by the NIT started with "00FF," which is a common MAC address used by virtual machines. (Doc. 94, PAGEID #604). Roden explained that "[a] virtual machine is a piece of software that runs on your computer that emulates another operating system and software applications." (Doc. 94, PAGEID #604). While Roden did not find evidence of a virtual machine on Defendant's laptop, there was evidence of a virtual machine on a desktop seized from Defendant's residence. (Doc. 94, PAGEID #614-615, 638). Special Agent Daniel Alfin testified that it was "self-evident that there was some type of either bridged network or virtual network adapter in use on the computer." (Doc. 94, PAGEID # 658). Alfin explained bridged network adapters as follows:

> So if you have on a particular computer multiple networks -- I believe we heard testimony of this particular computer had both a hard-wired network adapter as well as a wireless network adapter. There are certain applications where you may want to connect to multiple networks at a time and allow devices from those two networks to communicate with each other. So what you would do in that instance, or what you could do is create a virtual bridged network adapter.
>
> So this MAC address string here that begins with 00FF is commonly associated with virtualization applications, bridge networking applications. There is nothing here out of the ordinary to me. Nothing about this -- certainly nothing indicates that the NIT did not function as advertised.

(Doc. 94, PAGEID #658).

> Tor, your real IP address is invisible to the destination. So what the NIT does is it forces the computer to communicate outside of the Tor network over the regular internet. So when that happens, we can see the defendant's real IP address, and that's what occurred in this case. That is what's reflected in the two-way communication screen or PCAP data[2] that's been provided.

(Doc. 94, PAGEID # 655-56). It was the IP address which the FBI used to locate the user "billnyepedoguy" and obtain a search warrant for Defendant's home. Moreover, Alfin testified that:

> So we know what the exploit did in this case, and we know what the NIT did in this case. That entire communication, again, was recorded by the government and turned over in discovery. So if there was some other nefarious activity occurring here, it would have been recorded in that PCAP data stream. And the fact that it wasn't recorded in that data stream, it makes it clear that the exploit and the NIT did only what they were designed to do and nothing else.

(Doc. 94, PAGEID #663-64). Alfin disputed that any changes were made to Defendant's computer:

> The exploit doesn't make any changes to the computer. The way that I've described the exploit previously is: On the defendant's computer, there is an open window. He doesn't know about it, but the government does. So that open window is the exploit, and we send a NIT through it. The window was open when we got there. The window was open when we left. We didn't make any changes to the window. But everything that was done inside, all the evidence that was seized, just like any normal search warrant, we preserved all that data -- that's what the PCAP is -- and we turned it over in discovery.

(Doc. 94, PAGEID #665-66).

Next, Defendant points out that on March 4, 2015, the NIT reported that the operating system running on Defendant's computer was Windows 8.1. (Gov. Hr'g Ex. 1).

[2]Dr. Matthew Miller described the PCAP as "a capture of the network traffic that the government received." (Doc. 94, PAGEID #695).

However, when the government seized Defendant's laptop, the government reported the laptop was running a different version of Windows. (Def. Hr'g Ex. 7, at pp. 2, 5, 6).[3] The Government maintains that this discrepancy can be easily explained: Defendant upgraded his operating system after the dates of the NIT search -- February 20 to March 4, 2015 -- and before the seizure of Stamper's laptop in September of 2015. Indeed, Special Agent Doug Roden testified that on August 9, 2015, the operating system was changed when Windows 10 Enterprise was downloaded onto the computer. (Doc. 94, PAGEID #599).

Third, Defendant argues that eighty percent of the image files found on Defendant's laptop show "created dates" that were before February 3, 2015 – the date that Defendant purchased the hard drive which was installed in the laptop. (Def. Hrg. Exs. 4, 6A). Defendant explains that the created date is generally the date the image was saved to the hard drive. (Doc. 94, PAGEID #767). Defendant relies on the testimony of Dr. Matthew Miller that this discrepancy could indicate that the exploit had done damage to the computer and it was not keeping dates accurately. (See Doc. 94, PAGEID # 708-709).

The Court finds that this discrepancy in the time stamps is not a reliable indicator that the NIT was not functioning properly. Special Agent Roden testified that "timestamps can be a little tricky." (Doc. 94, PAGEID #605). Roden explained that operating systems have a time and that time can be changed "by simply clicking on the Time option and chang[ing] the date." (Doc. 94, PAGEID #605). Roden also explained

[3]The Court notes that there is some discrepancy about this discrepancy. Special Agent Roden testified that although his Report of Examination stated that Defendant's previous operating system was Windows Vista, that was an error. (Doc. 94. PAGEID #600-601).

that another source of time dates is the BIOS, which is a Basic Input/Output System. (Doc. 94, PAGEID #605-606). Roden also described situations where files that are "zipped" or bundled together will retain the original created or modified date. (Doc. 94, PAGEID #606). Roden summarized that "it's not a given that every file on a particular hard drive is within the time the computer was created or owned by that user." (Doc. 94, PAGEID #607). Moreover, Special Agent Alfin testified that the NIT did not have the capability to alter actual files contained on a person's computer. (Doc. 94, PAGEID #654). Instead, according to Special Agent Alfin:

> the NIT just operates or executes in memory on the computer. It doesn't write to the hard drive where files are stored. It doesn't remain in permanent storage on the computer. So anything pertaining to timestamps of files on a computer are completely independent of the NIT. They just -- they don't have anything to do with each other.

(Doc. 94, PAGEID #654).

The Court concludes that these discrepancies – either separately or as a whole – do not show that the exploit code is material because the exploit is not necessary to test reliability of the NIT.

Even if these errors showed the materiality of the exploit code, the Court would still not be persuaded that the Government should be compelled to produce this component of the NIT. The Government asserts that the law-enforcement privilege protects the exploit code. The Government argues that disclosure of the exploit would severely compromise future investigations, and could allow other individuals to develop countermeasures to avoid detection when violating the laws of the United States.

In determining whether the government is entitled to a law enforcement privilege,

this Court is to apply a balancing approach, weighing the government's concerns against the needs articulated by the defendant. *United States v. Pirosko*, 787 F.3d 358, 365 (6th Cir. 2015).

In *United States v. Pirosko,* 787 F.3d 358 (6th Cir. 2015), the Sixth Circuit concluded that a law enforcement privilege protected the requested FBI software from disclosure. The court distinguished the case before it from the facts of *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012). The Court explained that while the defendant in *Budziak* presented evidence of error in the operation of the software, the only evidentiary support provided by the defendant was a letter with one sentence questioning the government's affidavit because it does not show "which tools, which records, or the means by which those records were created" and "leaving otherwise answerable questions unanswered." 787 F.3d at 366. The Sixth Circuit concluded this "lone allegation is simply not enough to overcome the numerous facts supporting the government's position that it legitimately obtained child pornography from [the defendant]'s shared folders." *Id*. By way of explanation, the court stated:

> To be clear, this conclusion should not be read as giving the government a blank check to operate its file-sharing detection software sans scrutiny. As a general matter, it is important that the government's investigative methods be reliable, both for individual defendants like Pirosko and for the public at large. Still, we think that it is important for the defendant to produce some evidence of government wrongdoing.

Id.

Here, the Court concludes that Defendant has not shown sufficient evidence of wrongdoing to outweigh the Government's need to protect the information. Therefore, even if the Court were to conclude that the exploit code was material under Rule 16, the

Court would find that the exploit code is protected by the law enforcement privilege.

Accordingly, Defendant's Motions to Compel Discovery (Docs. 56, 79) are DENIED.

B. Motion for Reconsideration (Doc. 63)

Defendant asks this Court to reconsider its February 19, 2016 Order denying Defendant's Motion to Dismiss or Alternatively Suppress Evidence (Doc. 48).

As this Court has observed before, the Federal Rules of Criminal Procedure make no provision for a motion to reconsider. *United States v. Hopewell*, No. 1:08-cr-65, 2009 WL 1026452, at *1 (S.D. Ohio Apr. 15, 2009). Instead, "[c]ourts adjudicating such motions in criminal cases typically evaluate such motions under the same standards applicable to a civil motion to alter or amend judgment pursuant to Fed.R.Civ.P. 59(e)." *Id*. (quoting *United States v. Jarnigan*, No. 3:08–CR–7, 2008 WL 5248172, at *2 (E.D.Tenn. Dec.17, 2008)). "Under Rule 59, a court may alter the judgment based on: '(1) a clear error of law; (2) newly discovered evidence; (3) an intervening change in controlling law; or (4) a need to prevent manifest injustice.'" *Leisure Caviar, LLC v. U.S. Fish & Wildlife Serv*., 616 F.3d 612, 615 (6th Cir. 2010) (quoting *Intera Corp. v. Henderson*, 428 F.3d 605, 620 (6th Cir. 2005)). Here, Defendant ostensibly relies on an intervening change in controlling law.

In its February 19, 2016 Order, this Court denied suppression of the evidence the government obtained through the NIT warrant. Since that time, other judges from within this district have also denied motions to suppress in cases involving the same NIT warrant. *United States v. Spicer*, No. 1:15-cr-73, 2018 WL 635889, at *4 (S.D. Ohio Jan.

31, 2018); *United States v. Schuster*, No. 1:16-cr-51, 2017 WL 1154088, at *8 (S.D. Ohio Mar. 28, 2017); *United States v. Gaver*, 3:16-cr-088, 2017 WL 1134814, *12 (S.D. Ohio Mar. 27, 2017); *United States v. Jones*, No. 3:16-cr-026, 230 F. Supp.3d 819, 827 (S.D. Ohio Feb. 1, 2017).

A majority of the courts across the country which have been presented with the same issue have ruled similarly. These the decisions fall into two categories: (1) the NIT warrant violated Rule 41(b), or assuming without deciding that the warrant violated Rule 41(b), concluding that suppression was not warranted; or (2) the NIT warrant did not violate Rule 41(b) because it is a "tracking device" authorized by Rule 41(b)(4), but even if that were not the case, suppression is not warranted. *See United States v. Austin*, 230 F. Supp. 3d 828, 832 (M.D. Tenn. 2017) (collecting cases). A few courts fall within a third category, concluding that the NIT Warrant violated Rule 41(b), and ordered suppression as a remedy. *United States v. Levin*, 186 F.Supp.3d 26 (D. Mass. May 5, 2016); *United States v. Arterbury*, No. 15-cr-182 (N.D. Okla. April 25, 2016); *United States v. Workman*, 205 F.Supp.3d 1256, 2016 WL 5791209 (D. Colo. Sept. 6, 2016); *United States v. Croghan*, 209 F.Supp.3d 1080 (S.D. Iowa Sept. 19, 2016).

A number of federal circuit courts have also ruled on the suppression issue, reversing those decisions above which granted the motions to suppress. *See United States v. Levin*, 874 F.3d 316 (1st Cir. 2017) (reversing the lower court's finding that "the good-faith exception is inapplicable because the warrant at issue here was void ab initio"); *United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017) (reversing *Croghan* and finding the magistrate judge lacked jurisdiction to issue the NIT warrant, but the good faith

exception precluded suppression); and *United States v. Workman*, 863 F.3d 1313 (10th Cir. 2017) ("Even if the warrant had been invalid, the *Leon* exception would still apply.").

The Court cannot conclude in the face of the overwhelming majority of cases which have not found suppression warranted that it should reconsider its decision denying Defendant's Motion to Dismiss or Alternatively Suppress Evidence. Accordingly, Defendant's Motion for Reconsideration (Doc. 63) is DENIED.

C. Motion for *Franks* Hearing (Doc. 67)

Defendant seeks a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978) because the government made a false representation in the search warrant affidavit which was filed in support of the NIT warrant application. Defendant maintains that the NIT warrant would not have issued if the correct information had been provided.

To obtain a *Franks* hearing, a defendant must make a "substantial preliminary showing" that (i) the affidavit upon which a search warrant was granted contained a false statement made knowingly and intentionally or with a reckless disregard for the truth; and (ii) the allegedly false statement was "necessary to the finding of probable cause." *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978).

The affidavit attached to the NIT Warrant application described the Playpen website's home page logo as depicting "two images [of] partially clothed prepubescent females with their legs spread apart, along with the text underneath stating, 'No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out.'" (Doc. 33-1, NIT Search Warrant Aff. ¶ 12). The affidavit was signed by Special Agent Douglas Macfarlane on February 20, 2015. The NIT warrant was issued on that same

day by the magistrate judge in the Eastern District of Virginia.

It is undisputed that the Playpen homepage changed between February 18, 2015 and February 20, 2015. Special Agent Macfarlane was present and testified on this same issue at a hearing before another judge in this district. *See United States v. Gaver*, No. 3:16-cr-88, 2017 WL 1134814, at *5 (S.D. Ohio Mar. 27, 2017). The change to the home page was summarized in the written opinion in *Gaver*:

> Paragraph 12 of Macfarlane's February 20, 2015, affidavit describes the homepage of the Play Pen website as follows: "On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart." Gov't Ex. 1. At the hearing, Macfarlane testified that this was the logo that appeared every time he viewed the homepage from September of 2014 through February 18, 2015. He did not access the site again between February 18, 2015, and February 20, 2015, when he submitted the warrant application. Hr'g Tr. at 72-76.
>
> It is undisputed that, sometime in that two-day period, the logo was changed. On February 20, 2015, the homepage showed just one girl, perhaps slightly older than the girls previously depicted, wearing a short dress, fishnet stockings and posed in a sexually suggestive manner. Ex. C. Although one of the other agents may have signed onto the website on February 19, 2015, and observed this change, no one told Macfarlane about it. Hr'g Tr. at 75.

2017 WL 1134814, at *5.

In *Gaver*, this Court found that the defendant had not shown that the false statement was made knowingly and intentionally, or with reckless disregard for the truth. *Id*. This Court observed: "Given that the logo had remained unchanged for months, [Macfarlane's] failure to access the website one last time prior to submitting the affidavit may have been somewhat negligent, but it cannot be deemed reckless." *Id*. This Court also explained: "in the Court's view, the old logo and the new logo are not materially

different." This Court noted: "As the other courts have found, both logos are highly suggestive of the website's illegal contents, particularly when paired with the website's name, and the fact that it was accessible only through the Tor network." *Id*. at *6 (citing *United States v. Matish*, 193 F. Supp. 3d 585, 606 (E.D. Va. 2016); *United States v. Darby*, 190 F. Supp. 3d 520, 534 (E.D. Va. 2016); *United States v. Allain*, 213 F. Supp. 3d 236, 247 (D. Mass. 2016); *United States v. Owens*, No. 16-cr-38, 2016 WL 7079609, at *6 (E.D. Wis. Dec. 5, 2016)). This Court finds no error in this reasoning, and also concludes that even if Macfarlane had accurately described the homepage, there still would have been probable cause for the search.

Accordingly, Defendant's Motion for a *Franks* Hearing (Doc. 67) is DENIED.

III. CONCLUSION

Based on the foregoing, Defendant's Motions to Compel Discovery (Docs. 56, 79) are **DENIED**; Defendant's Motion for Reconsideration (Doc. 63) is **DENIED**; and Defendant's Motion for a *Franks* Hearing (Doc. 67) is **DENIED**.

IT IS SO ORDERED.

/s/ Michael R. Barrett
Michael R. Barrett, Judge
United States District Court